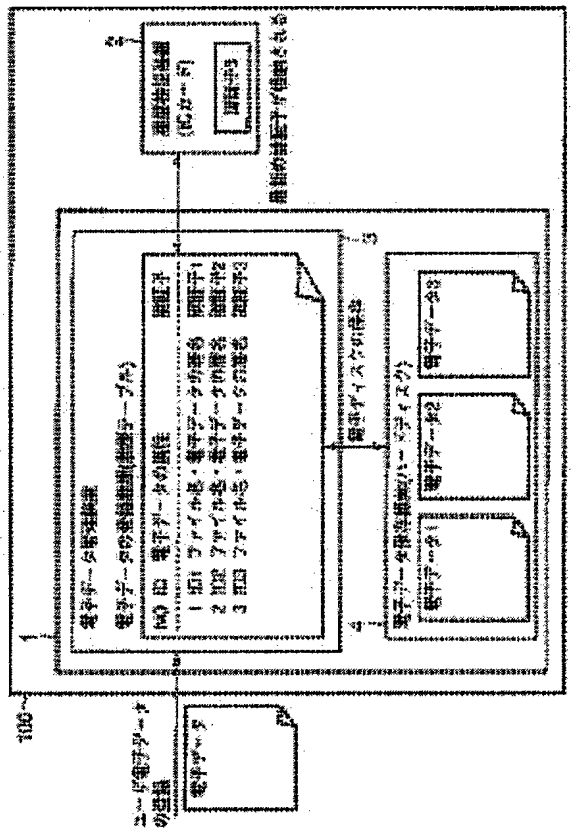
ELECTRONIC DATA STORAGE SYSTEM, HISTORY VERIFYING DEVICE, ELECTRONIC DATA STORING METHOD AND RECORDING MEDIUM

Publication number: JP2001337600 (A)
Publication date: 2001-12-07
Inventor(s): NISHIZAWA HIDEKAZU
Applicant(s): TOKYO SHIBAURA ELECTRIC CO
Classification:
- international: ***G06F12/14; G06F12/00; G06F17/30; G06F21/24; G06K19/10; G09C1/00;*** **G06F12/14; G06F12/00; G06F17/30; G06F21/00; G06K19/10; G09C1/00;** (IPC1-7): G09C1/00; G06F12/00; G06F12/14; G06F17/30; G06K19/10
- European:
Application number: JP20000158728 20000529
Priority number(s): JP20000158728 20000529

Abstract of **JP 2001337600 (A)**

PROBLEM TO BE SOLVED: To provide an electronic data storage system, a history verifying device, an electronic data storing method and a recording medium by which electronic data can be prevented from being fraudulently altered or erased and detecting erasure and alteration of electronic data and capable of securing the original record performance of the electronic data can be secured.; SOLUTION: In this system 100 which has a history management device 5 for managing the history of stored electronic data and a history verifying device 2 which has a means for detecting the alteration of the history and a means for verifying that the history is the newest history and stores and manages the electronic data, the history management device 5 has a means for confirming that individual histories are not fraudulently altered, a means which prepares an identifier for verifying that the time sequential relation of histories is not fraudulently altered and verifies the relation. The history verifying device 2 stores the identifier of the newest history in the inside and a means 18 for verifying whether or not the verifier of the inside is matched with the identifier of the newest history of the history table.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－337600
（P2001－337600A）
(43)公開日　平成13年12月７日(2001.12.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*(参考)
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｂ０１７
			６４０Ｄ	５Ｂ０３５
Ｇ０６Ｆ　12/00	５３７	Ｇ０６Ｆ　12/00	５３７Ｚ	５Ｂ０７５
12/14	３１０	12/14	３１０Ｚ	５Ｂ０８２
17/30	１２０	17/30	１２０Ａ	５Ｊ１０４

審査請求　未請求　請求項の数８　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2000－158728(P2000－158728)

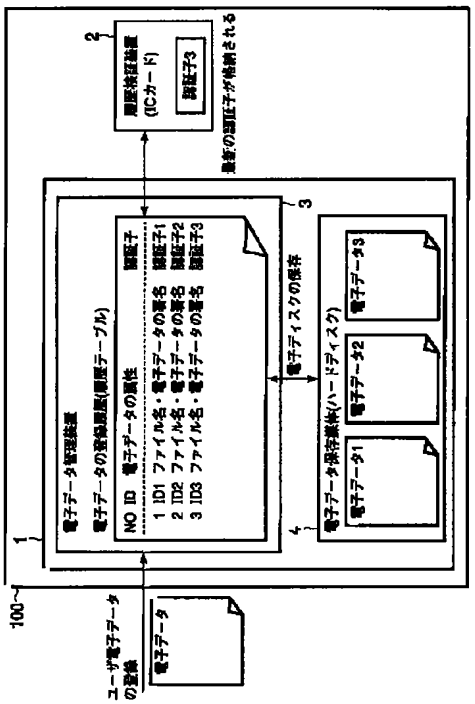
(22)出願日　平成12年５月29日(2000.5.29)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　西澤　秀和
東京都府中市東芝町１番地　株式会社東芝府中工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B017 AA07 CA16
5B035 AA15 BB09
5B075 KK54 KK66
5B082 AA01 FA11 GA11
5J104 AA08 LA03 LA05 NA35 NA38
PA14

(54)【発明の名称】　電子データ保管システム、履歴検証装置、電子データ保管方法及び記録媒体

(57)【要約】
【課題】電子データの改ざん、消去の防止及び検知を可能にするとともに、電子データの原本性を確保することのできる電子データ保管システム、履歴検証装置、電子データ保管方法及び記憶媒体を提供すること。
【解決手段】電子データ保管の履歴を管理する履歴管理装置５と、履歴に対する改ざんを検知する手段および前記履歴が最新の履歴であることを検証する手段とを有した履歴検証装置２とを有した電子的なデータを保管し管理するシステム１００において、履歴管理装置５は個々の履歴が改ざんされていないことを確認する手段と、履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための手段を有する。また履歴検証装置２は、最新の履歴の検証子を内部に保管し、内部の認証子と、履歴テーブルの最新の履歴の認証子が一致するか否かを検証する手段１８を有する。



【特許請求の範囲】
【請求項１】　電子的なデータを保管し管理する電子データ保管システムにおいて、
電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置と、履歴検証装置とから構成され、
前記履歴管理装置は、
個々の履歴が改ざんされていないことを確認する確認手段と、
履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、を具備し、
前記履歴検証装置は、
個々の履歴に対する改ざんを検知する改ざん検知手段と、
最新の履歴の認証子を内部に保管し、前記内部に保管された認証子と前記履歴テーブルの最新の履歴の認証子の一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を具備することを特徴とする電子データ保管システム。
【請求項２】　前記履歴検証装置は、前記最新の履歴の認証子を格納する最新認証子格納庫と、
履歴の更新と認証子を作成する認証子更新手段と、を備え、
前記最新認証子格納庫は外部からのアクセスが不可能であるように構成され、前記認証子更新手段により正当な手順を経て履歴が更新された場合にのみ前記最新認証子格納庫に格納された最新の認証子を更新することを特徴とする請求項１記載の電子データ保管システム。
【請求項３】　前記履歴検証装置は、前記履歴テーブルの履歴が改ざんされていないことを検証するための認証子検証手段を備え、
前記認証子検証手段は、前記履歴テーブルの最新の履歴の認証子と前記最新認証子格納庫の認証子が一致するか検証することを特徴とする請求項１記載の電子データ保管システム。
【請求項４】　電子的なデータを保管し管理する電子データ保管システムにおいて、
電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置と、最新の履歴の認証子を内部に保管する履歴検証装置と、から構成され、前記履歴管理装置は、個々の履歴が改ざんされていないことを確認する確認手段と、
個々の履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、
個々の履歴に対する改ざんを検知する改ざん検知手段と、
前記履歴検証装置から、最新の履歴の認証子を読み出し前記履歴テーブルの最新の履歴の認証子との一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を具備することを特徴とする電子データ保管システム。
【請求項５】　電子データの保管に際し、
電子データ保管の履歴の時系列の関係が改ざんされていないことを検証するための認証子の作成と、電子データが改ざんされていないことを検証するためのメッセージ認証子の作成とを行うための履歴検証装置にアクセスし、履歴の認証子及び電子データのメッセージ認証子を受け取る手順と、
履歴が改ざんされてなく、また最新の履歴であることを検証するために、前記履歴検証装置にアクセスし、検証結果を受け取る手順と、
を実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。
【請求項６】　電子データ保管の履歴を記憶する履歴テーブルにおける個々の履歴が改ざんされていないことを確認する手順と、
履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成する手順と、
最新の履歴の認証子を内部に保管する履歴検証装置から最新の履歴の認証子を読み出し、前記履歴テーブルの最新の履歴の認証子との一致を検証することにより前記履歴が最新の履歴であることを検証する手順と、を実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。
【請求項７】　電子データ保管の履歴を管理する履歴管理装置と、履歴に対する改ざんを検知する手段と、前記履歴が最新の履歴であることを検証する手段を備えた履歴検証装置とから構成される、電子的なデータを保管し管理するシステムにおける電子データ保管方法において、
前記履歴管理装置は、履歴番号、識別子、属性情報、メッセージダイジェスト、及び前記履歴番号、識別子、属性情報、メッセージダイジェストのメッセージダイジェストを暗号化して得られる認証子から成る履歴情報を前記履歴検証装置に送信し、
前記履歴検証装置は、
前記履歴管理装置から送信された履歴番号、識別子、属性情報、メッセージダイジェスト及び認証子を受信し、これらの情報からメッセージダイジェストを作成し、
前記作成したメッセージダイジェストと１つ前の認証子との排他的論理和をとり、
前記履歴管理装置から送信された認証子を復号化し、前記排他的論理和により得られる値と比較し、
前記比較の結果、一致が得られたとき、前記履歴管理装置から送信された履歴情報が最新の履歴情報か否か判断し、
前記最新の履歴情報であるとき、前記履歴管理装置から送信された認証子と前記履歴検証装置内の最新認証子格納庫に保管されている最新認証子とを比較し、その比較

結果を前記履歴管理装置に送信する、ことを特徴とする電子データ保管方法。

【請求項８】　電子的データ保管の履歴を管理する履歴管理装置と、履歴が最新の履歴であることを検証するための最新認証子を最新認証子格納庫に保管する履歴検証装置とから構成される、電子的なデータを保管し管理するシステムにおける電子データ保管方法において、

前記履歴管理装置は、

履歴番号、識別子、属性情報、メッセージダイジェスト、及び前記履歴番号、識別子、属性情報、メッセージダイジェストのメッセージダイジェストを暗号化して得られる認証子からなる履歴情報にもとづいてメッセージダイジェストを作成し、

前記作成したメッセージダイジェストと１つ前の認証子との排他的論理和をとり、

前記暗号化された認証子を復号化し、前記排他的論理和により得られる値と比較し、前記比較の結果、一致が得られたとき、前記履歴情報が最新の履歴情報か否か判断し、

前記最新の履歴情報であるとき、前記履歴検証装置内の最新認証子格納庫から最新認証子を読み出し、前記履歴情報の認証子と比較し、履歴の時系列の関係が改ざんされているか否かを検証する、ことを特徴とする電子データ保管方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は電子データの改ざん、消去の防止および検知を可能とするとともに、電子データの原本性を確保する電子データ保管システム、履歴検証装置、電子データ保管方法および記憶媒体に関する。

【０００２】

【従来の技術】新しい通信技術が導入されるとともにインターネットが爆発的に普及するにつれ、情報のセキュリティをいかに確保するかが重要な課題となっている。例えば、WWW(World Wide Web)サーバとブラウザ間でのセキュリティは、第三者によるデータの盗聴、改ざんの防止や第三者のなりすましによる被害を防止し、安全にデータのやり取りが行える環境を提供することにある。このためには、ネットワーク上を流れるデータを保護するために次の三つの機能を実現する必要ある。

【０００３】すなわち、（１）ブラウザが通信している相手が本当のサーバーであること（第三者によるなりすましのサーバーでないこと）を保証するためのサーバー確認(Authentication)、（２）第三者によるデータの盗聴を防止するために転送するデータの暗号化(Encryption)、および（３）データの転送中にデータが改ざんされずに相手に送られたことを保証するデータ一貫性の保証(Data Integrity)の機能である。

【０００４】サーバー認証は、電子証明書と公開鍵暗号方式を用いて実現される。電子証明書は、サーバーの名前（ドメイン名）やサーバーの公開鍵、電子証明書の有効期間、電子証明書の認証機関の情報等のサーバーの身分を証明する情報とそれらの情報が正しいことを保証する電子署名から構成される（図２０参照）。電子署名はサーバの情報を基に作成され、認証機関の秘密鍵で暗号化される（図２１参照）。サーバーはこの電子証明書をブラウザ側に送ることにより、ブラウザが電子署名を復号して得られた情報と、証明書の内容を比較し、内容が一致すれば本当に正しいサーバーと通信していることが証明される。

【０００５】この仕組みは電子証明書に書かれている内容が正しい情報であることが前提となっている。このため、ＣＡ(Certificate Authorities)と呼ばれる認証機関が、証明書の請求に応じて、電子証明書を発行するように構成される。

【０００６】

【発明が解決しようとする課題】上述したように、電子データ改ざん検知のために電子署名が用いられるが、従来は電子データ保管の履歴が改ざんされているか否かを検出する手段が無かったために、電子署名の付けられたデータについて、それが最新の改訂版なのか、すでに破棄されている過去の版のコピーなのか区別がつかず、電子データの原本性の保証ができないという問題があった。

【０００７】本発明は上記事情に鑑みてなされたもので、その目的は、電子データの改ざん、消去の防止及び検知を可能にするとともに、電子データの原本性を確保することのできる電子データ保管システム、履歴検証装置、電子データ保管方法及び記録媒体を提供することである。

【０００８】

【課題を解決するための手段】（１）本発明の電子データ保管システム（請求項１）は、電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置であって、個々の履歴が改ざんされていないことを確認する確認手段と、履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、を備えた履歴管理装置と、履歴に対する改ざんを検知する改ざん検知手段と、最新の履歴の認証子を内部に保管し、前記内部に保管された認証子と前記履歴テーブルの最新の履歴の認証子の一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を備えた履歴検証装置、とを具備することを特徴とする。

【０００９】本発明によれば、電子データの改ざん、消去の防止および検知が可能となるとともに、電子データの原本性が確保される。

【００１０】（２）好ましくは（請求項２）、前記履歴検証装置は、前記最新の履歴の認証子を格納する最新認

証子格納庫と、履歴の更新と認証子を作成する認証子更新手段と、を備え、前記最新認証子格納庫は外部からのアクセスが不可能であるように構成され、前記認証子更新手段により正当な手順を経て履歴が更新された場合にのみ前記最新認証子格納庫に格納された最新の認証子を更新することを特徴とする。

【００１１】（３）好ましくは（請求項３）、前記履歴検証装置は、前記履歴テーブルの履歴が改ざんされていないことを検証するための認証子検証手段を備え、前記認証子検証手段は、前記履歴テーブルの最新の履歴の認証子と前記最新認証子格納庫の認証子が一致するか検証することを特徴とする。

【００１２】（４）本発明の電子データ保管システム（請求項４）は、電子的なデータを保管し管理する電子データ保管システムにおいて、最新の履歴の認証子を内部に保管する履歴検証装置と、電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置であって、個々の履歴が改ざんされていないことを確認する確認手段と、履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、履歴に対する改ざんを検知する改ざん検知手段と、前記履歴検証装置から、最新の履歴の認証子を読み出し前記履歴テーブルの最新の履歴の認証子との一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を備えた履歴管理装置と、を具備することを特徴とする。

【００１３】（５）請求項５に対応する発明は、請求項１に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００１４】（６）請求項６に対応する発明は、請求項９に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００１５】本願発明によれば、電子保管の個々の履歴の排他的論理和をとり、それにより得られる最新の認証子を例えばＩＣカードのような耐タンパー性を有する装置に保管される。この最新の認証子は情報が不正に改ざんされることを防ぐため、装置の機能により正当なプロセスを経た場合にのみ、情報の更新が行われ、外部からの情報への直接のアクセスは一切不可である。これによりシステムの構成を簡単化することができる。この点につき、従来は電子データ保管システム全体を安全な装置に入れ、電子データ自体は例えばハードディスク装置に入れ装置外部に設けるが、履歴の管理装置はシステムの中に入っていて外部から不正にアクセスできないような構成になっている。このためシステム全体を収めるための耐タンパー性を有した箱を設ける必要がありコストがかさむという問題点を本願発明は解決することができる。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００１７】図１は本発明の実施の形態における電子データ保管システムの基本的な構成である。電子データ保管システム１００はサーバ計算機１と履歴検証装置２とから構成される。サーバ計算機１は電子データ管理装置３と電子データ保存媒体４を有する。履歴検証装置２は電子データの原本性を保証する上で核となる装置であり、耐タンパー性を備えたハードウエアから構成される。具体的には、ＩＣカード等が考えられる。電子データ管理装置３は特定の機能を備えたハードウエア、またはソフトウエアをインストールした計算機から構成される。電子データ管理装置３は電子データを保管・管理するためのインターフェース機能を有する。

【００１８】図２は、本発明の電子データ保管システム１００の概略図である。ユーザは電子データ保管システム１００内の電子データ管理装置３に電子データ（電子文書等）を登録する。電子データ保管システム１００は電子データの管理を行う電子データ管理装置３と、電子データが格納される、例えばハードディスク装置から構成される電子データ保存媒体４、及び例えばＩＣカードにより実現される履歴検証装置２とから構成される。ここで、ユーザにより登録された電子データは電子署名等の認証情報がつけられて電子データ保存媒体４に格納される。このとき、電子データ管理装置３内にある履歴テーブルに、登録行為の情報が記載される。履歴テーブルはその真正性を保証するために認証子がつけられており、履歴が最新であることを保証するため、履歴の最新行の認証子（ここでは、認証子３）がシステムに装着された履歴検証装置（ＩＣカード等に）２に安全に保管される。

【００１９】図３は電子データ保存媒体４に格納される電子データＤ１の形態を示す。電子データ保存媒体４は電子データ管理装置３によって電子データＤ１の書き込み、読み出しが行われる。電子データ保存媒体４には電子データＤ１に添付情報Ｄ２が関連づけて格納される。添付情報Ｄ２は、電子データを一意に識別するためのID、作成者・日付等の属性情報、内容が改ざんされていないことを保証するためのメッセージ認証子が含まれる。IDは文書番号と改訂番号からなり、新規文書が保存されるたびに文書番号が更新されていく。改訂版の保存の場合には、文書番号は同一で改訂番号を更新する。

【００２０】図４は電子データ管理装置３の構成を示す。電子データ管理装置３は履歴管理装置５、履歴検証装置アクセス装置６、メッセージダイジェスト作成装置７、メッセージ認証子検証装置８、電子データ管理装置制御装置９からなり、電子データ保存機能Ｆ１、電子データ検証機能Ｆ２を備え、これらの機能によりユーザは電子データの保管・管理を行う。メッセージダイジェスト作成装置７はメッセージダイジェスト作成機能Ｆ３を備え、電子データＤ１のメッセージ認証子作成に必要な

メッセージダイジェストを作成する。メッセージダイジェストは例えばハッシュ法を用いて作成される。メッセージ認証子検証装置８はメッセージ認証子検証機能Ｆ４を備え、電子データＤ１が改ざんされていないかを検証する。履歴検証装置アクセス装置６は履歴管理装置５からの処理要求を受け取り、履歴検証装置２へ送信する。履歴検証装置２の処理結果は履歴検証装置アクセス装置６を経て履歴管理装置５に返される。電子データ管理制御装置９はユーザからの要求入力を受け取り、各種の機能を実行する。

【００２１】図５は履歴管理装置５の構成を示す。履歴管理装置５は履歴テーブル格納庫１０と履歴管理制御装置１１からなり、識別子発番機能Ｆ５、履歴検証機能Ｆ６、履歴登録機能Ｆ７をもつ。履歴テーブル格納庫１０は電子データの保存の履歴を格納し、履歴管理制御装置１１は電子データ管理制御装置９からの要求を受付け、各種の機能を実行し、その結果を返す。

【００２２】図６は履歴テーブル格納庫１０に格納される履歴の形態を示す。履歴は履歴番号、識別子、属性情報、電子データのメッセージダイジェスト、認証子を列とする表形式からなる。

【００２３】図７は履歴と認証子の関係を示している。認証子は履歴テーブルの内容が改ざんされていないことを検証するためにつけられる。最初の履歴について、履歴番号１番と電子データの識別子、属性情報、メッセージダイジェスト２１から新たにメッセージダイジェスト２３を作成する。作成されたメッセージダイジェスト２３は暗号化され認証子１となる。図７でＥは暗号化の処理を表す。なお、メッセージダイジェスト２１は登録する電子データのメッセージダイジェストであって、登録する電子データが改ざんされているか否かを検証するためのものであり、メッセージダイジェスト２３は履歴のメッセージダイジェストであり、履歴が改ざんされているか否かを検証するのに用いる。２番目以降の履歴に関しては、同様に作成されたメッセージダイジェストと直前の認証子との排他的論理和をとってから暗号化を行う。これにより履歴の一部が改ざんされる、あるいは履歴の順番が変更された場合には、認証子の整合性が取れなくなり、履歴が改ざんされたことが検知できる。さらに履歴の最新行の認証子を履歴検証装置２内に安全に保管することにより、履歴が最新の情報であることを保証する。

【００２４】図８は履歴検証装置２の構成を示す。履歴検証装置２は電子データ用復号化鍵格納庫１２、電子データ用暗号化鍵格納庫１３、履歴用復号化鍵格納庫１４、履歴用暗号化鍵格納庫１５、最新認証子格納庫１６、最新履歴番号格納庫１７、履歴検証制御装置１８からなり、認証子更新機能Ｆ８、認証子検証機能Ｆ９、履歴の認証子検証機能Ｆ１０を備える。履歴検証装置２は電子データの原本性を保証する上で重要な情報を保持しており、情報が不正に改ざんされることを防ぐため、装置の機能により正当なプロセスを経た場合にのみ、情報の更新が行われ、外部からの情報への直接のアクセスは一切不可であるとする。また、電子データ用復号化鍵格納庫１２、電子データ用暗号化鍵格納庫１３、履歴用復号化鍵格納庫１４、履歴用暗号化鍵格納庫１５は一度情報を書き込んだ後は二度と書き込み、変更は不可である。履歴検証装置２の機能は認定を行う団体によって検査されたのち、各種の鍵が各鍵格納庫１２乃至１５に書き込まれる。さらに最新認証子格納庫１６に初期コード（例えば０の羅列からなるコード）を、また最新履歴暗号格納庫１７には０をそれぞれセットする。鍵、初期コード、初期値を書き込まれた履歴認証装置は認定団体によって認定・登録される。履歴検証制御装置１８は履歴検証装置アクセス装置６を経由して機能実行要求を受け取り、処理結果を返す。

【００２５】以下に各装置の機能を述べる。図９は電子データ管理装置３において、電子データ保存機能Ｆ１を実行したときのフローチャートを示す。電子データ保存機能Ｆ１では電子データＤ１、及び属性情報Ｄ４を入力として得る。改訂番の保存の場合には、さらに文書番号Ｄ５を入力として得る。始めにステップＳ１で、履歴管理装置５の後述する履歴検証機能Ｆ６を実行する。エラーが返された場合にはステップＳ９でエラーメッセージを出力し、終了する。すでに履歴の検証がなされ、履歴に改ざんのないことが確認されている場合には、このステップを外すことは可能である。ステップＳ１が正常に終了した場合には、ステップＳ３で履歴管理装置５の後述する識別子発番機能Ｆ５を実行し、新たな識別子Ｄ６を取得する。改訂番の場合には、文書番号Ｄ５を入力として識別子発番機能Ｆ５に渡す。エラーが返された場合には、ステップＳ９に進み、終了する。ステップＳ３が正常に終了した場合には、ステップＳ５でメッセージダイジェスト作成装置７のメッセージダイジェスト作成機能Ｆ３に電子データＤ１、属性情報Ｄ４、識別子Ｄ６を入力として与え、メッセージダイジェストＤ７を受け取る。次に、ステップＳ６で履歴管理装置５の後述する履歴登録機能Ｆ７に識別子Ｄ６、属性情報Ｄ４、メッセージダイスジェトＤ７を入力として与える。エラーが返された場合は、ステップＳ９に進みエラーメッセージを出力して終了する。ステップＳ６が正常に終了した場合、メッセージ認証子Ｄ８を出力として得る。識別子Ｄ６と属性情報Ｄ４とメッセージ認証子Ｄ８をまとめて添付情報Ｄ２として、電子データＤ１と関連づけして電子データ保存媒体４に格納し、終了する。

【００２６】図１０は電子データ管理装置３において、電子データ検証機能Ｆ２を実行したときのフローチャートを示す。入力として検証する電子データＤ１の識別子Ｄ６を受け取る。始めにステップＳ１０において、履歴管理装置５の履歴検証機能Ｆ６を実行する。ステップＳ

１０が正常に終了した場合には、ステップＳ１２において電子データ保存媒体４から識別子Ｄ６に対応する電子データＤ１とその添付情報Ｄ２を読み出し、ステップＳ１３において電子データＤ１とその添付情報Ｄ２を入力としてメッセージ認証子検証装置８のメッセージ認証子検証機能Ｆ４を実行する。エラーが返された場合には、ステップＳ１５に進み、終了する。ステップＳ１３が正常に終了した場合には終了する。

【００２７】メッセージ認証子検証機能Ｆ４はメッセージダイジェスト作成装置７のメッセージダイジェスト作成機能Ｆ３に電子データＤ１と添付情報Ｄ２から取り出した属性情報Ｄ４、識別子Ｄ６を入力として与え、メッセージダイジェストＤ７を受け取る。次に、履歴検証装置アクセス装置６を経由して履歴検証装置２の履歴の認証子検証機能Ｆ１０にメッセージダイジェストＤ７及び添付情報Ｄ２から取り出したメッセージ認証子Ｄ８を入力として与え、実行する。履歴の認証子検証機能Ｆ１０は電子データ用復号化鍵格納庫１２に格納された鍵を用いて、メッセージ認証子を復号化し、得られたコードがメッセージダイジェスト２３と等しいか検証する。等しくなければ履歴検証装置２はエラーメッセージを電子データ管理装置３に返す。メッセージ認証子検証装置８のメッセージ認証子検証機能Ｆ４は、履歴検証装置２の履歴の認証子検証機能Ｆ１０がエラーを返した場合には、エラーを返し、それ以外は正常終了する。

【００２８】図１１は履歴管理装置５において、識別子発番機能Ｆ５を実行したときのフローチャートを示す。入力データとして、文書番号Ｄ５が与えられた場合には、改訂版の発番ということでステップＳ２１に進む。文書番号Ｄ５が与えられない場合は、新規文書の発番ということでステップＳ１７に進む。ステップＳ１７では、履歴テーブル格納庫１０を検索し、最新の文書番号を得る。これをｂとすると、ステップＳ１８においてｂに１を加えて新たに文書番号を得る。これをｂ’とする。ステップＳ１９で改訂番号をｒ＝０とし、ステップＳ２０で新たな識別子ＩＤ＝（ｂ’，ｒ）（識別子Ｄ６）を出力し、終了する。改訂版の発番の場合には、ステップＳ２１においてｂ＝文書番号Ｄ５とする。次にステップＳ２２で履歴テーブル格納庫１０を検索し、文書番号Ｄ５と等しい文書番号の識別子が存在するか確認する。存在しない場合には、不当な文書番号を入力されたということでステップＳ２７に進み、エラーメッセージを出力して終了する。ステップＳ２２が正常に終了した場合には、ステップＳ２４に進み、履歴テーブル格納庫１０を検索し、文書番号Ｄ５に対して最新の改訂番号（識別子内に含まれる）を得る。これをｒとする。ステップＳ２５においてｒに１を加えてあらたに改訂番号を得る。これをｒ’とする。ステップＳ２６で新たな識別子Ｄ６＝（ｂ，ｒ’）を出力し、終了する。

【００２９】図１２は履歴管理装置５において、履歴検証機能Ｆ６を実行したときのフローチャートを示す。始めにステップＳ２８で履歴テーブル格納庫１０の履歴の行数を調べ、これをＫで表す。又、変数としてｋを用意し、ｋ＝１とする。次に、ステップＳ２９において履歴テーブル格納庫１０のｋ番目の行から、履歴番号Ｄ９、識別子Ｄ１０、属性情報Ｄ１１、メッセージダイジェストＤ１２、認証子Ｄ１３を読み出す。ステップＳ３０においてｋ＝１の場合にはステップＳ３２に進む。それ以外の場合はステップＳ３１において履歴テーブル格納庫１０のｋ－１番目の行から認証子Ｄ１４を読み出す。ステップＳ３２において、履歴番号Ｄ９、識別子Ｄ１０、属性情報Ｄ１１、メッセージダイジェストＤ１２、認証子Ｄ１３、ｋ＝１でない場合にはさらに認証子Ｄ１４を入力として履歴検証装置２の認証子検証機能Ｆ９を実行する。エラーが返された場合には履歴が改ざんされたものとしてステップＳ３６に進み、エラーメッセージを出力して終了する。ステップＳ３２が正常に終了した場合にはステップＳ３４において、ｋ＝Ｋであるか調べる。ｋ＝Ｋであれば処理を終了する。ｋ＝ＫでなければステップＳ３５においてｋに１を加え、ステップＳ２９に戻る。

【００３０】図１３は履歴管理装置５において、履歴登録機能Ｆ７を実行したときのフローチャートを示す。履歴登録機能Ｆ７では、識別子Ｄ６、属性情報Ｄ４、メッセージダイジェストＤ７を入力として受け取る。始めにステップＳ３７で履歴テーブル格納庫１０を検索し、識別子Ｄ６が重複しないことを確認する。重複している場合には不正な識別子としてステップＳ４２に進み、エラーメッセージを出力して終了する。ステップＳ３７が正常に終了した場合（識別子が重複していない場合）は、ステップＳ３９に進み、識別子Ｄ６、属性情報Ｄ４、メッセージダイジェストＤ７を入力として履歴検証装置２の認証子更新機能Ｆ８を実行し、履歴番号Ｄ１５、識別子Ｄ６、メッセージ認証子Ｄ８を出力として受け取る。ステップＳ４１で履歴テーブル格納庫１０に履歴番号Ｄ１５、識別子Ｄ６、属性情報Ｄ４、メッセージダイジェストＤ７、認証子Ｄ１６を新たな行に追加する。ステップＳ４２でメッセージ認証子Ｄ８を出力し、終了する。

【００３１】図１４は履歴検証装置２において、認証子更新機能Ｆ８を実行したときのフローチャートを示す。認証子更新機能Ｆ８は識別子Ｄ６、属性情報Ｄ４、メッセージダイジェストＤ７を入力として得る。始めにステップＳ４４で最新履歴番号格納庫１７の履歴番号をＫとする、Ｋに１を加え、K+1とする。これを新たな履歴番号Ｄ１５とする。ステップＳ４５で履歴番号Ｄ１５、識別子Ｄ６、属性情報Ｄ４、メッセージダイジェストＤ７から新たにメッセージダイジェストＤ１６を生成する。ステップＳ４６において、履歴番号Ｄ１５が１であるか否か調べ、１の場合はステップＳ４８に進む。１でない場合はステップＳ４７に進み、メッセージダイジェスト

Ｄ１６と最新認証子格納庫１６に格納されている最新の認証子Ｄ１７との排他的論理和を取り、コードＤ１８を得たのち、ステップＳ４８に進む。ステップＳ４８ではコードＤ１８またはメッセージダイジェストＤ１６を履歴用暗号化鍵格納庫１５に格納されている暗号化鍵により暗号化し、新たな認証子Ｄ１６を生成する。ステップＳ４９では新たな認証子Ｄ１６を最新認証子格納庫１４に格納する。ステップＳ５０で入力データのメッセージダイジェストＤ７を、電子データ用暗号化鍵格納庫１３に格納されている暗号化鍵により暗号化しメッセージ認証子Ｄ８を生成する。ステップＳ５１で履歴番号Ｄ１５、認証子Ｄ１６、メッセージ認証子Ｄ８を出力し、終了する。

【００３２】図１５は、履歴検証装置２において、認証子検証機能Ｆ９を実行した時のフローチャートを示す。認証子検証機能Ｆ９は入力として履歴番号Ｄ９、識別子Ｄ１０、属性情報Ｄ１１、メッセージダイジェストＤ１２、認証子Ｄ１３を、履歴番号Ｄ９が１でない場合にはさらに認証子Ｄ１４を得る。ステップＳ５２において、履歴番号Ｄ９、識別子Ｄ１０、属性情報Ｄ１１、メッセージダイジェストＤ１２からメッセージダイジェストＤ１９を作成する。ステップＳ５３において、履歴番号Ｄ９が１の場合はステップＳ６１において、メッセージダイジェストＤ１９をコードＤ２０として、ステップＳ５５に進む。それ以外の場合は、ステップＳ５４において、メッセージダイジェストＤ１９と１つ前の認証子Ｄ１４との排他的論理和をとり、コードＤ２０を得たのち、ステップＳ５５に進む。ステップＳ５５で認証子Ｄ１３を履歴用復号化鍵格納庫１２の復号化鍵で復号化しコードＤ２１を得る。ステップＳ５６においてコードＤ２０またはメッセージダイジェストＤ１９とコードＤ２１が等しいか否かを検証する。等しくなければ、履歴は改ざんされたものとしてステップＳ６０へ進み、エラーメッセージを出力して終了する。等しければステップＳ５７に進み、履歴番号Ｄ９が最新履歴番号格納庫１５の履歴番号Ｄ１５と等しいか否か調べる。等しくなければ終了し、等しければ、ステップＳ５８に進む。ステップＳ５８では認証子Ｄ１３が最新認証子格納庫１４の最新の認証子Ｄ１６と等しいか否か検証する。等しければ終了し、等しくなければ履歴が最新のものでないということでステップＳ６０へ進み、エラーメッセージを出力して終了する。

【００３３】図１６は履歴管理装置と履歴検証装置２との間のデータのやりとりを図式化したものである。なお、図１５と同一部には同符号を付す。履歴管理装置５は履歴テーブル１０内履歴番号、識別子、属性情報、メッセージダイジェスト、現在の認証子（Ｄ１３）、１つ前の認証子（Ｄ１４）を履歴検証装置２に送る。

【００３４】履歴検証装置２はステップＳ５２において、履歴管理装置５から送られた、履歴番号、識別子、属性情報、メッセージダイジェストのメッセージダイジェストを作成する。次に、ステップＳ５４において、作成したメッセージダイジェストと１つ前の認証子Ｄ１４との排他的論理和をとる。そして、ステップＳ５５において、認証子Ｄ１３を復号化し排他的論理和により得られる値と比較する。ステップＳ５６において、比較結果が不一致であれば、履歴検証装置２はその旨を示すエラーメッセージを履歴管理装置５に返す。一方、比較結果が一致する場合には、ステップＳ５７において、履歴が最新の履歴か否か判断する。最新の履歴でない場合には、履歴検証装置２は、履歴が改ざんされていない旨のメッセージを履歴管理装置５に送る。一方、最新の履歴の場合には、さらに認証子Ｄ１３と最新認証子格納庫内の最新認証子が等しいか否か判断する。等しくない場合には、その旨を示すエラーメッセージを履歴管理装置５に返し、等しい場合には、履歴の時系列の時系列の関係が改ざんされていない旨の通知を履歴管理装置５に返す。

【００３５】なお、本発明は上記実施の形態に限定されない。例えば、電子データ用復号化鍵と履歴用復号化鍵、及び電子データ用暗号化鍵と履歴用暗号化鍵はそれぞれ同一でもよい。その場合には、履歴用復号化鍵格納庫１４及び履歴用暗号化鍵格納庫１５は省略してもよい。

【００３６】また、暗号処理は共通鍵暗合方式でも公開鍵暗合方式でもよい。公開鍵暗号方式の場合には図１７に示すように、履歴管理装置５の内部に電子データ復号化鍵格納庫１２と履歴用復号化鍵格納庫１４を備える。

【００３７】電子データの検証を行うには、メッセージ認証子検証装置８のメッセージ認証子検証機能Ｆ４において、履歴管理装置５の電子データ用復号化鍵格納庫１２に格納された鍵を用いて、メッセージ認証子を復号化し、得られたコードがメッセージダイジェストと等しいか検証する。

【００３８】履歴の検証を行うには、履歴管理装置５で図１２に示すフローチャートと図１５に示すフローチャートの両方を実行する。このときのフローチャートは図１８に示すようになる。図１８では、ステップＳ５８－Ａにおいて、認証子が最新であることを検証するため、履歴検証装置２から最新認証子を読み出し履歴テーブル１０の認証子と比較を行う。他は図１２および図１５と基本的に同じである。

【００３９】図１９は履歴管理装置５側において、履歴の検証を行う場合の履歴管理装置５と履歴検証装置２との間のデータのやりとりを図式化したものである。なお、図１２および図１５と同一部には同符号を付す。

【００４０】履歴管理装置５はステップＳ２８において、履歴テーブルのｋ番目の行を読む。次に、ステップＳ３１において、ｋ－１番目の行から認証子Ｄ１４を読む。次に、ステップＳ５２において、履歴番号、識別

子、属性情報、メッセージダイジェストのメッセージダイジェストを作成する。ステップＳ５４において、作成したメッセージダイジェストと１つ前の認証子Ｄ１４との排他的論理和を取る。ステップＳ５５において、認証子Ｄ１３を復号化し排他的論理和により得られる値と比較し、不一致であれば、エラーメッセージを出力する。一方、一致すれば、ステップＳ５７において、履歴が最新の履歴か否か判断する。最新の履歴でなければ、ステップＳ２８に戻る。一方、最新の履歴であれば、履歴管理装置５は履歴検証装置２内の最新認証子格納庫１６内の最新認証子を読み出し、認証子Ｄ１３と等しいか否か判断する（ステップＳ５８（Ｓ５９））。等しくなければ、その旨を示すフローチャートを出力し、等しければ履歴の時系列の関係が改ざんされていない旨の通知を出力する。

【００４１】この場合には認証子の検証の大部分を履歴管理装置５で行うことで、履歴検証装置２の負担を減らすことができる。

【００４２】また、電子データ管理システム１００の運用方法によっては、履歴検証装置２の機能に対する団体の認定は省略できる。

【００４３】

【発明の効果】この発明によれば、電子データを保管し管理する装置に、電子データ保存の履歴を記録する履歴テーブルと、履歴テーブルに対する改ざんの有無を検知するための認証情報を作成する手段と、履歴テーブルが最新であることを認証するための履歴検証手段と、認証情報を安全に管理する履歴検証装置を備える構成としたので、電子データの改ざん、消去を防止することができるとともに、電子データの原本性を確保することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態における電子データ保管システムの基本的な構成を示すブロック図である。

【図２】本発明一実施の形態における電子データ保管システムの概略図である。

【図３】上記実施の形態における電子データ保存媒体に格納される電子データＤ１の形態図である。

【図４】上記実施の形態における電子データ管理装置の構成を示すブロック図である。

【図５】上記実施の形態における履歴管理装置の構成を示すブロック図である。

【図６】上記実施の形態における履歴テーブル格納庫に格納される履歴の形態図である。

【図７】上記実施の形態における履歴と認証子の関係を示す図である。

【図８】上記実施の形態における履歴検証装置の構成を示すブロック図である。

【図９】上記実施の形態における電子データ管理装置において、電子データ保存機能Ｆ１の処理を示すフローチャートである。

【図１０】上記実施の形態における電子データ管理装置において、電子データ検証機能Ｆ２の処理を示すフローチャートである。

【図１１】上記実施の形態における履歴管理装置において、識別子発番機能Ｆ５の処理を示すフローチャートである。

【図１２】上記実施の形態における履歴管理装置において、履歴検証機能Ｆ６の処理を示すフローチャートである。

【図１３】上記実施の形態における履歴管理装置において、履歴登録機能Ｆ７の処理を示すフローチャートである。

【図１４】上記実施の形態における履歴検証装置において、認証子更新機能Ｆ８の処理を示すフローチャートである。

【図１５】上記実施の形態における履歴検証装置において、認証子検証機能Ｆ９の処理を示すフローチャートである。

【図１６】上記実施の形態において、履歴管理装置５と履歴検証装置２との間のデータのやりとりを示すフローチャートである。

【図１７】本発明の第２の実施の形態における電子データ保管システムのブロック図である。

【図１８】図１２において、認証子の検証機能を履歴検証装置の外部で行うときの処理を示すフローチャートである。

【図１９】上記第２の実施の形態において、履歴管理装置５と履歴検証装置２との間でデータのやりとりを示すフローチャートである。

【図２０】電子証明書の構造を示す説明図である。

【図２１】サーバー認証の仕組みを示す説明図である。

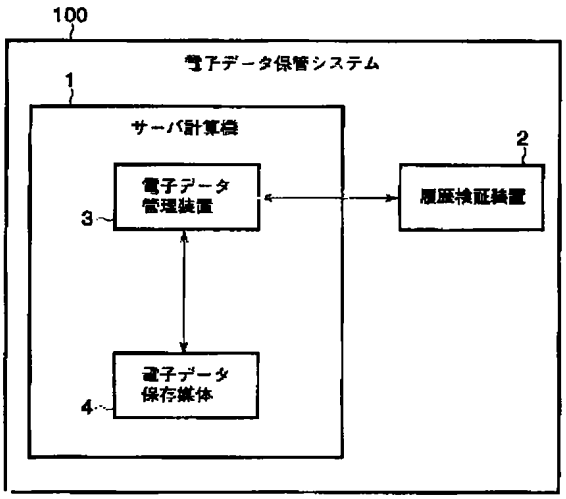
【符号の説明】

１…サーバ計算機
２…履歴検証装置
３…電子データ管理装置
４…電子データ保存媒体
５…履歴管理装置
６…履歴検証装置アクセス装置
７…メッセージダイジェスト作成装置
８…メッセージ認証子検証装置
９…電子データ管理制御装置
１０…履歴テーブル格納庫
１１…履歴管理制御装置
１２…電子データ用復号化鍵格納庫
１３…電子データ用暗号化鍵格納庫
１４…履歴用復号化鍵格納庫
１５…履歴用暗号化鍵格納庫
１６…最新認証子格納庫
１７…最新履歴番号格納庫

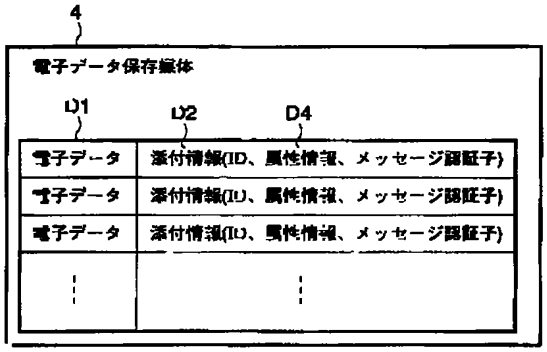
１８…履歴検証制御装置

１００…電子データ保管システム

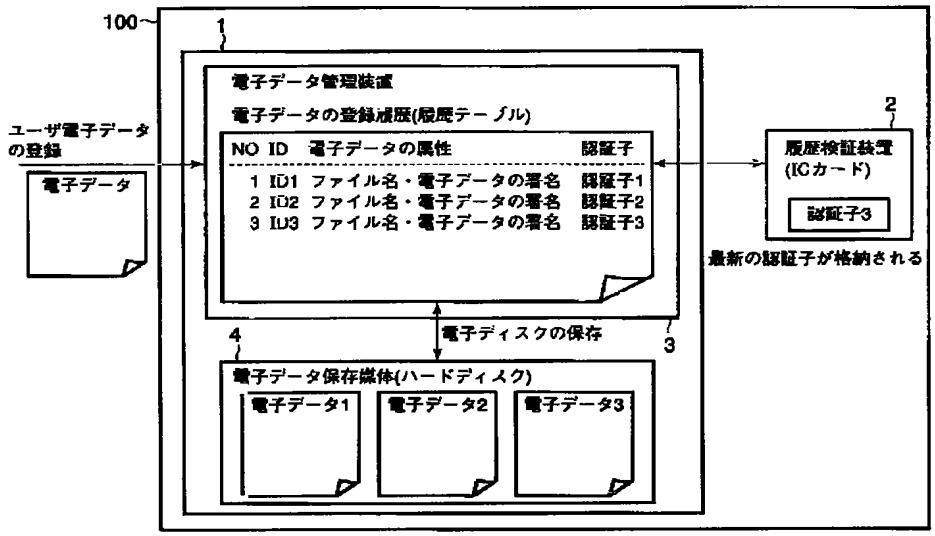
【図１】



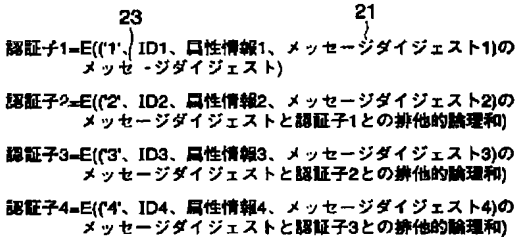
【図３】



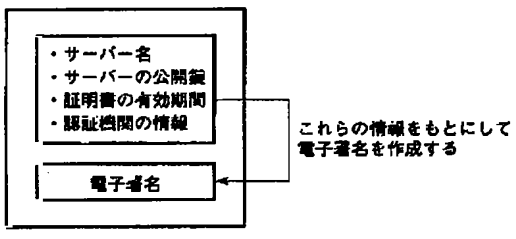
【図２】



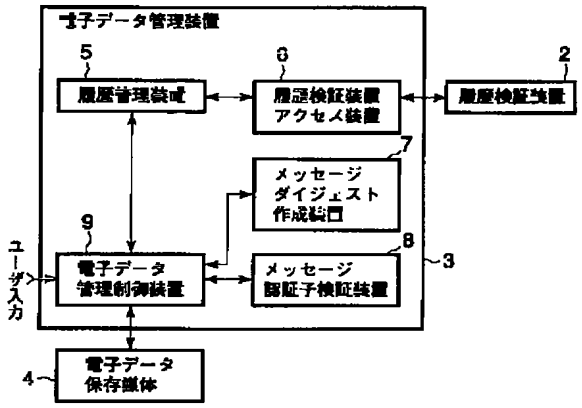
【図７】



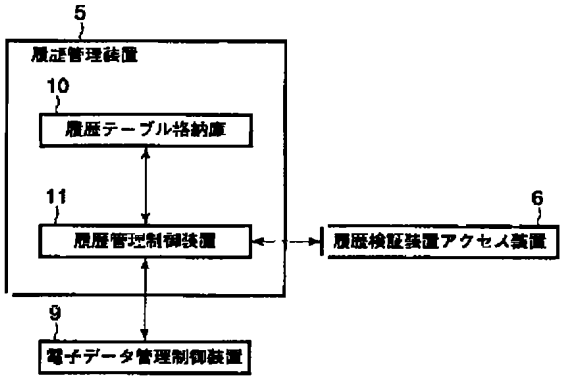
【図２０】



【図4】



【図5】



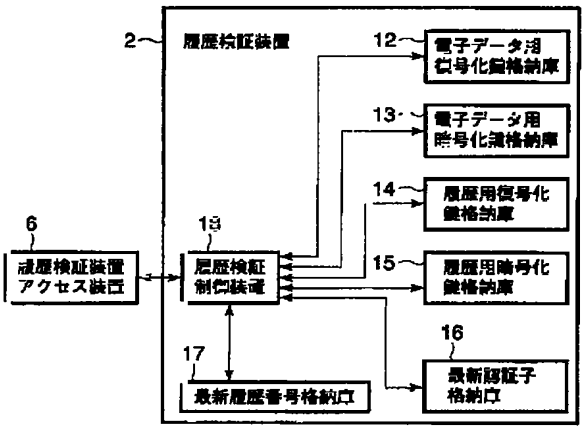
【図6】

10

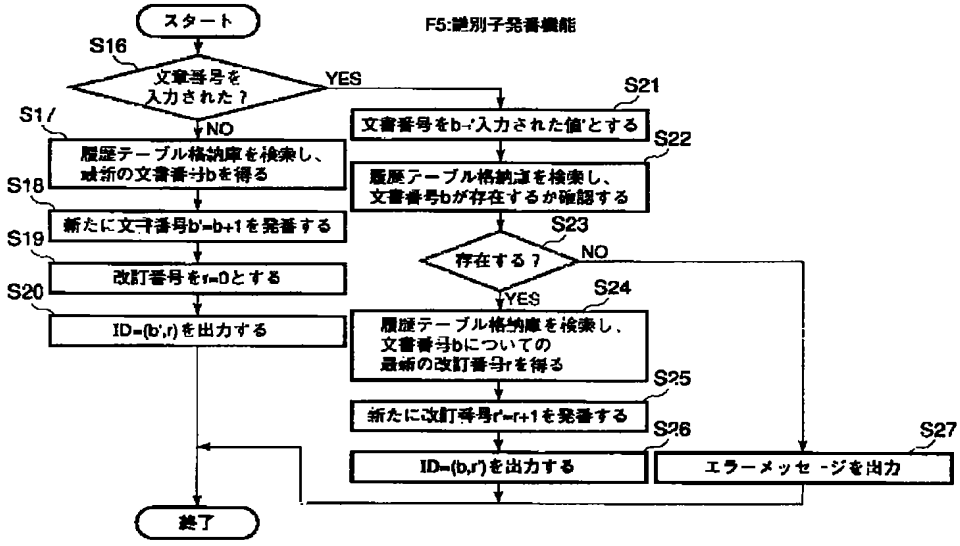
履歴テーブル格納庫

1	ID1	属性情報1	MD1	認証子1
2	ID2	属性情報2	MD2	認証子2
3	ID3	属性情報3	MD3	認証子3
⋮	⋮	⋮	⋮	⋮

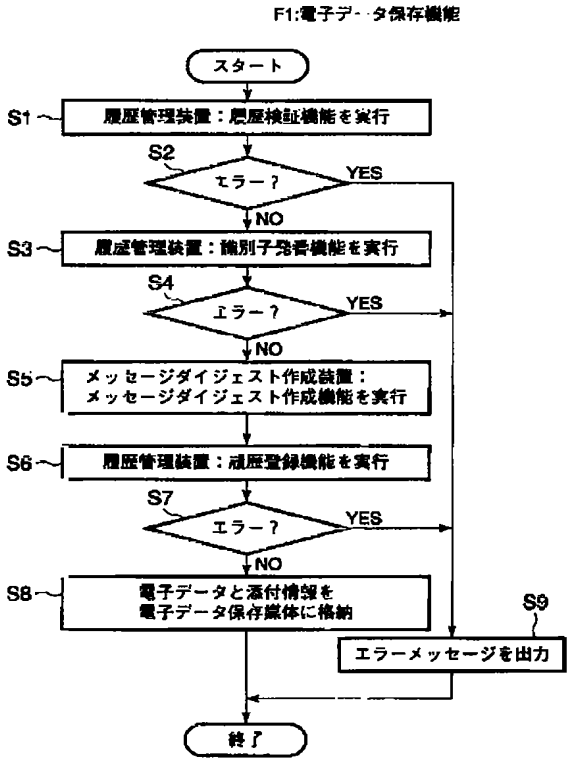
【図8】



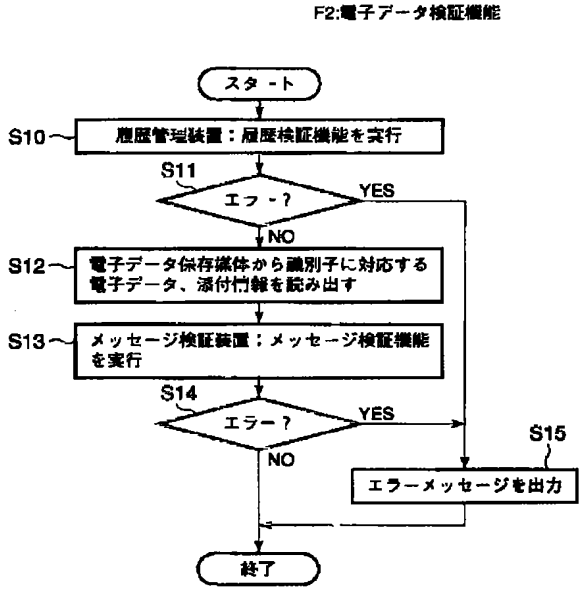
【図11】



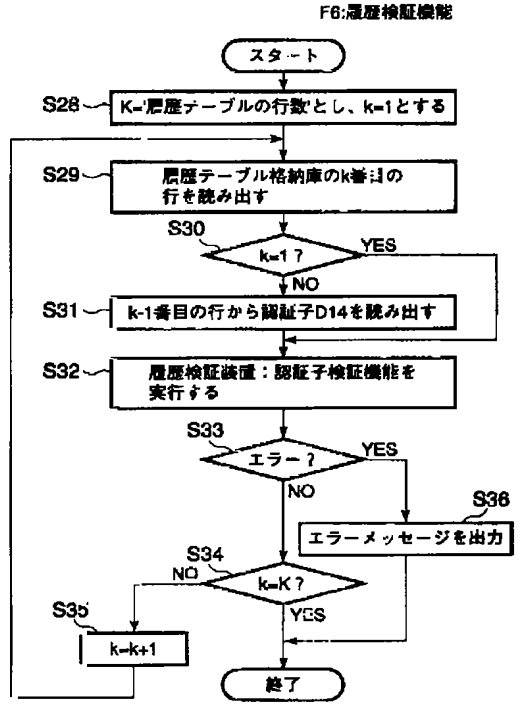
【図９】



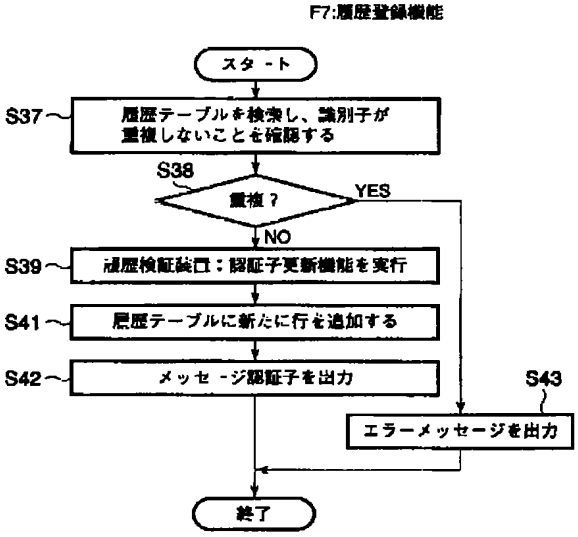
【図１０】



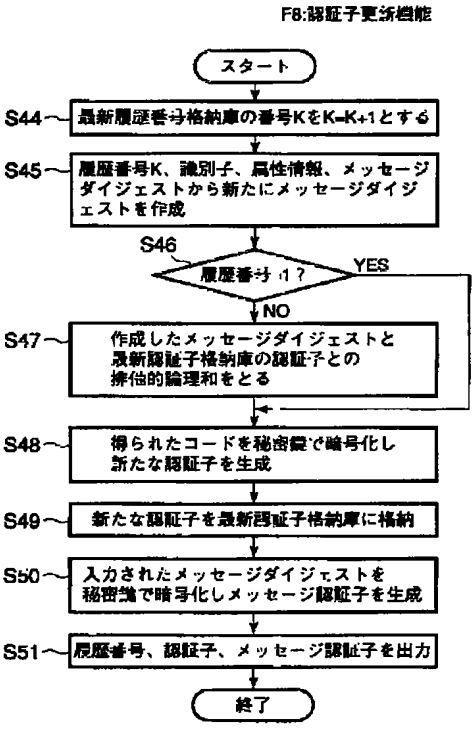
【図１２】



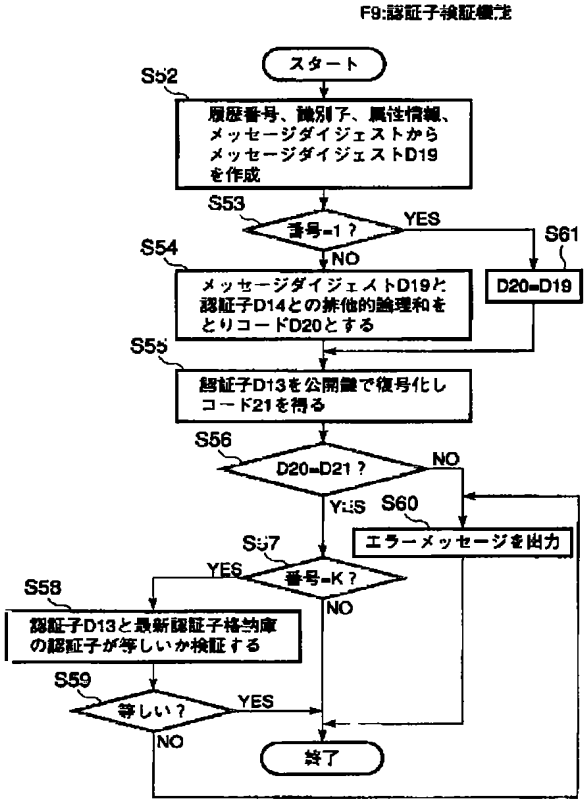
【図１３】



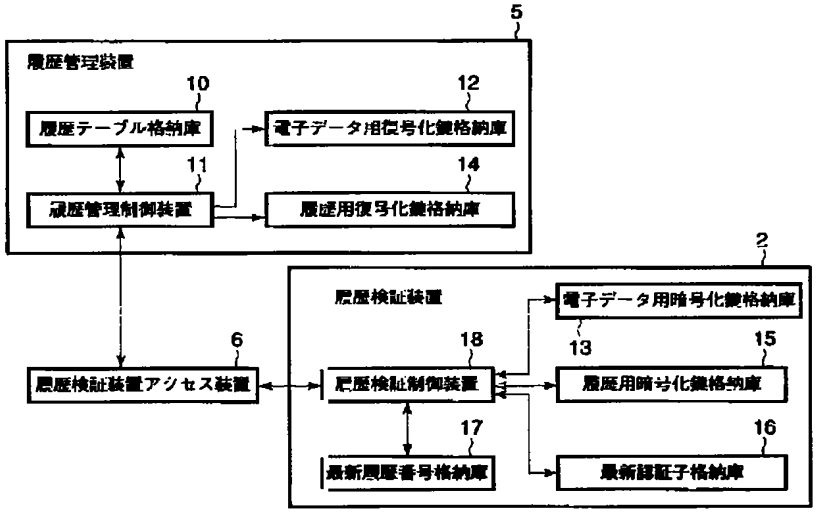
【図14】


F8:認証子更新機能
スタート
S44
最新履歴番号格納庫の番号KをK=K+1とする
S45
履歴番号K、識別子、属性情報、メッセージダイジェストから新たにメッセージダイジェストを作成
S46
履歴番号=1？
YES
NO
S47
作成したメッセージダイジェストと最新認証子格納庫の認証子との排他的論理和をとる
S48
得られたコードを秘密鍵で暗号化し新たな認証子を生成
S49
新たな認証子を最新認証子格納庫に格納
S50
入力されたメッセージダイジェストを秘密鍵で暗号化しメッセージ認証子を生成
S51
履歴番号、認証子、メッセージ認証子を出力
終了

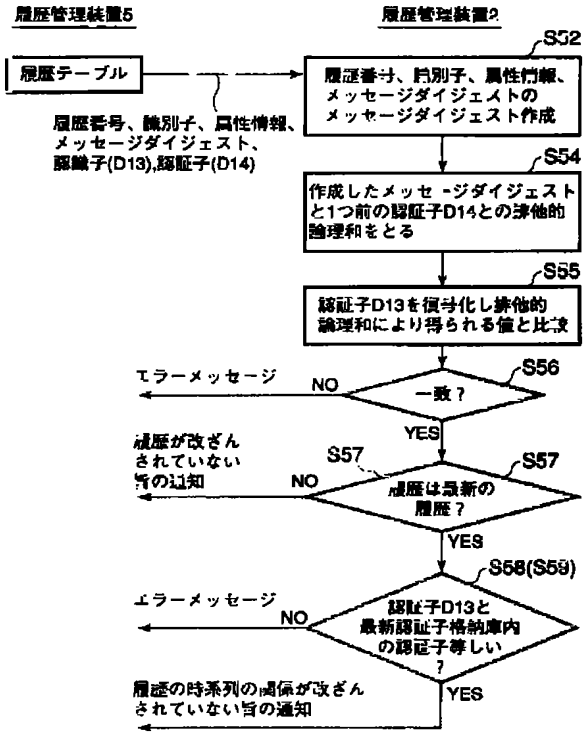
【図15】


F9:認証子検証機能
スタート
S52
履歴番号、識別子、属性情報、メッセージダイジェストからメッセージダイジェストD19を作成
S53
番号=1？
YES
NO
S61
D20=D19
S54
メッセージダイジェストD19と認証子D14との排他的論理和をとりコードD20とする
S55
認証子D13を公開鍵で復号化しコード21を得る
S56
D20=D21？
NO
YES
S60
エラーメッセージを出力
S57
番号=K？
YES
NO
S58
認証子D13と最新認証子格納庫の認証子が等しいか検証する
S59
等しい？
YES
NO
終了

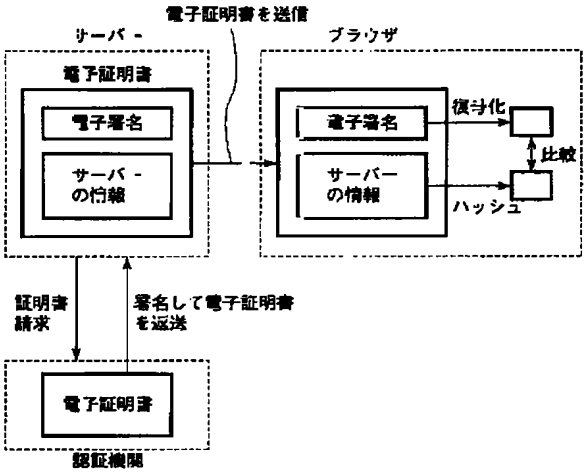
【図17】


5
履歴管理装置
10
履歴テーブル格納庫
12
電子データ用復号化鍵格納庫
11
履歴管理制御装置
14
履歴用復号化鍵格納庫
2
履歴検証装置
電子データ用暗号化鍵格納庫
6
履歴検証装置アクセス装置
18
履歴検証制御装置
13
15
履歴用暗号化鍵格納庫
17
16
最新履歴番号格納庫
最新認証子格納庫

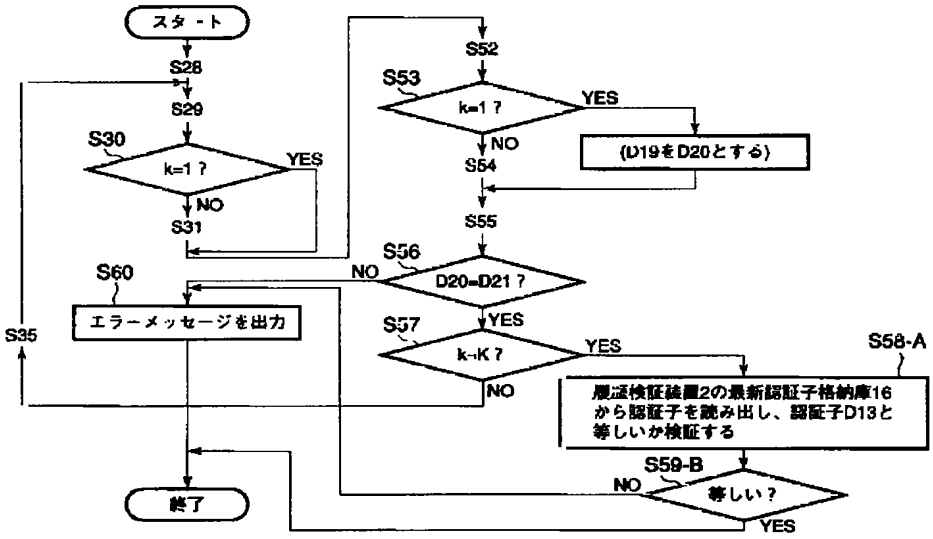
【図16】


履歴管理装置5
履歴管理装置2
履歴テーブル
履歴番号、識別子、属性情報、
メッセージダイジェスト、
認証子(D13),認証子(D14)
S52
履歴番号、識別子、属性情報、
メッセージダイジェストの
メッセージダイジェスト作成
S54
作成したメッセージダイジェスト
と1つ前の認証子D14との排他的
論理和をとる
S55
認証子D13を復号化し排他的
論理和により得られる値と比較
S56
一致？
エラーメッセージ
NO
YES
S57
履歴は最新の
履歴？
履歴が改ざん
されていない
旨の通知
NO
S57
YES
S58(S59)
認証子D13と
最新認証子格納庫内
の認証子等しい
？
エラーメッセージ
NO
YES
履歴の時系列の関係が改ざん
されていない旨の通知

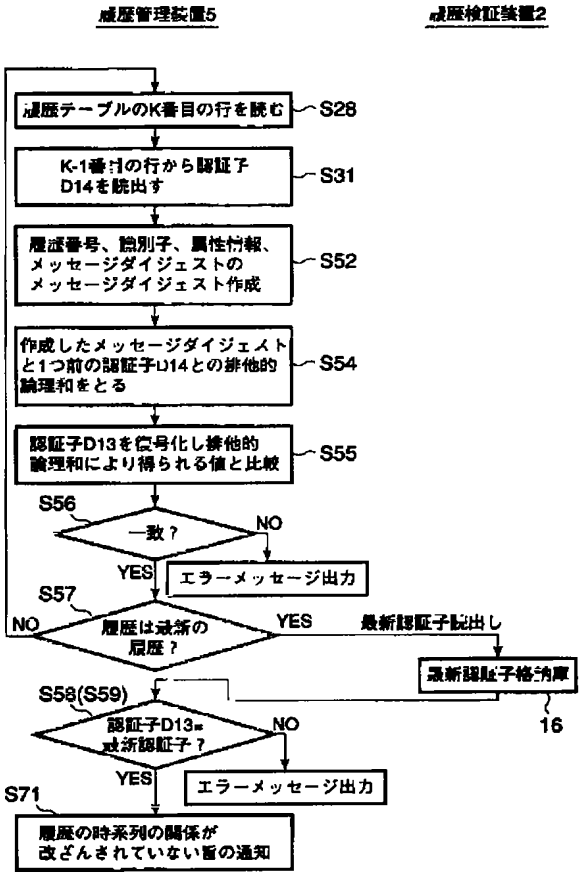
【図21】


電子証明書を送信
サーバ
ブラウザ
電子証明書
電子署名
サーバの情報
電子署名
サーバーの情報
復号化
比較
ハッシュ
証明書
請求
署名して電子証明書
を返送
電子証明書
認証機関

【図18】


スタート
S28
S29
S30
k=1？
YES
NO
S31
S52
S53
k=1？
YES
NO
(D19をD20とする)
S54
S55
S56
D20=D21？
NO
YES
S57
k=K？
YES
NO
S58-A
履歴検証装置2の最新認証子格納庫16
から認証子を読み出し、認証子D13と
等しいか検証する
S59-B
等しい？
NO
YES
S60
エラーメッセージを出力
S35
終了

【図19】



フロントページの続き

(51)Int.Cl.⁷	識別記号	FI	(参考)
G06K 19/10		G06K 19/00	R